WHAT IS CLAIMED IS:

1. A secure electronic document, comprising:

a form for entry of a password by a recipient of the document, the form being adapted to be displayed within an HTML-compliant web browser;

an encrypted message; and

a decryption module that uses the password to decrypt the encrypted message for display within the HTML-compliant web browser;

wherein the document allows the encrypted message to be decrypted and viewed on a computer having an HTML-compliant browser installed thereon, without a need for decryption software installed on the computer.

2. The secure electronic document of Claim 1 wherein the form is configured to present a password entry field and a decryption button to a user when the form is processed by the HTML-compliant web browser.

3. The secure electronic document of Claim 1 wherein the encrypted message comprises an email attachment.

4. The secure electronic document of Claim 1 wherein the decryption module comprises script code configured to be executed within the HTML-compliant browser.

5. The secure electronic document of Claim 4 wherein the decryption module comprises JavaScript commands.

6. The secure electronic document of Claim 4 wherein the decryption module comprises a set of Visual Basic script commands.

7. The secure electronic document of Claim 1 wherein the decryption module is configured to receive a password and use the password to generate a decryption key, the decryption module being configured to use the decryption key to decrypt the encrypted message.

8. The secure electronic document of Claim 1 wherein the decryption module comprises an Active X control.

9. The secure electronic document of Claim 1 wherein the decryption module comprises software which is configured to be executed within a browser.

10. The secure electronic document of Claim 1 wherein the decryption module is downloaded across a communications medium as needed.

11. The secure electronic document of Claim 1 wherein the decryption module comprises a Java applet.

12. The secure electronic document of Claim 1 where the decryption module comprises both a Java program and an Active X control.

13. A secure electronic document comprising:

a document wrapper including a description of a user interface;

encrypted data representing a source message which has been encrypted with an encryption key;

processing instructions located within the document wrapper; and

a decryption element configured to receive a password entered by a recipient via the user interface, and to use the password and the processing instructions to decrypt the encrypted data within the document.

14. The secure electronic document of Claim 13 wherein the document wrapper is formatted in Hyper Text Markup Language.

15. The secure electronic document of Claim 13 wherein the document wrapper is formatted in Extensible Markup Language.

16. The secure electronic document of Claim 13 wherein the document wrapper is configured to present a password entry field and a decryption button to a user when the wrapper is processed by a browser.

17. The secure electronic document of Claim 13 wherein the processing instructions are executed in response to a user clicking the decryption button.

18. The secure electronic document of Claim 17 wherein the processing instructions are configured to send data from the password entry field to the decryption element.

19. The secure electronic document of Claim 13 wherein the encrypted data comprises an email attachment.

20. The secure electronic document of Claim 17 wherein the processing instructions comprise script code configured to be executed within a browser.

21. The secure electronic document of Claim 20 wherein the processing instructions comprise JavaScript commands.

22. The secure electronic document of Claim 20 wherein the processing instructions comprise a set of Visual Basic script commands.

23. The secure electronic document of Claim 13 wherein the decryption element is configured to receive a password and use the password to generate a decryption key, the decryption element being configured to use the decryption key to decrypt the encrypted data and recover the source message.

24. The secure electronic document of Claim 13 wherein the decryption element comprises at least one of either a set of Visual Basic script commands and a set of JavaScript commands.

25. The secure electronic document of Claim 13 wherein the decryption element comprises an Active X control.

26. The secure electronic document of Claim 13 wherein the decryption element comprises software which is configured to be executed within a browser.

27. The secure electronic document of Claim 26 wherein the decryption element is downloaded across a communications medium as needed.

28. The secure electronic document of Claim 26 wherein the decryption element comprises a Java applet.

29. The secure electronic document of Claim 26 where the decryption element comprises both a Java program and an Active X control.

30. A secure messaging system for protecting the contents of an electronic message being sent to a recipient, the system comprising:

an encrypting module for preparing a secure document, the encrypting module configured to receive a key and an electronic message; and

an electronic mail gateway module configured to receive the secure document from the encrypting module and to send the secure document to a recipient,

wherein the encrypting module is configured to create an encrypted message by encrypting the electronic message with the key, and wherein the secure document comprises an HTML-compliant wrapper, the encrypted

message, a processing script, and a decryption element, the processing script containing instructions for accessing the encrypted message, and the decryption element being capable of recovering the electronic message from the encrypted message when presented with a password by the recipient.

31. The secure messaging system of Claim 30 wherein the decryption element is configured to send a confirmation message to the encrypting module confirming the successful access of the encrypted message by the recipient.

32. The secure messaging system of Claim 31 wherein the confirmation message allows the sender to identify the recipient of the message.

33. A method for sending a message to a recipient, the method comprising the steps of:

preparing an encrypted message by encrypting a source message using an encryption key and an encryption algorithm;

preparing a secure document comprising an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element, wherein the processing script contains instructions for accessing the encrypted message, and wherein the decryption element includes a module capable of recovering the source message from the encrypted message when presented with a password by the recipient; and

sending the secure document to a recipient.

34. The method for sending a message of Claim 33 wherein the source message is received as part of an XML template.

35. The method for sending a message of Claim 33 wherein the encryption key is derived from the password.

36. The method for sending a message of Claim 35 wherein the password is hashed to generate the encryption key.

37. The method for sending a message of Claim 33 wherein the password is received as part of an XML template.

38. A method for sending and receiving a message, the method comprising the steps of:

preparing an encrypted message by encrypting a source message using an encryption key associated with a recipient and an encryption algorithm;

preparing a secure document comprising an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element;

forwarding the secure document to a recipient's device;

processing the wrapper of the secure document using a browser running on the recipient's device;

entering a password into the browser;

running the processing script of the secure document to access the decryption element;

recovering the source message by decrypting the encrypted message with the password and the decryption element; and

presenting the recovered source message to the recipient,

wherein the secure document allows the encrypted message to be decrypted and viewed on a device having a browser installed thereon, without a need for decryption software installed on the device.

39. The method for sending a message of Claim 38 wherein the source message is received as part of an XML template.

40. The method for sending a message of Claim 38 wherein the encryption key is derived from the password.

41. The method for sending a message of Claim 40 wherein the password is hashed to generate the encryption key.

42. The method for sending a message of Claim 38 wherein the password is received as part of an XML template.

43. A computer readable medium having stored therein a software module, which when executed performs the steps of:

preparing an encrypted message by encrypting a source message using an encryption key and an encryption algorithm;

preparing a secure document comprising an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element, wherein the processing script contains instructions for accessing the encrypted message,

and wherein the decryption element includes a module capable of recovering the source message from the encrypted message when presented with a password by the recipient;

forwarding the secure document to a mail gateway module.